CLAIMS

What is claimed is:

1. A method of providing location privacy, comprising:

for a mobile computing device, assigning a pool of addresses with which a user can access a network, and preventing a third party from correlating a user's location with the mobile computing device.

2. The method of claim 1, wherein said addresses comprise media access control (MAC) addresses.

3. The method of claim 1, wherein said pool of addresses is assigned by a manufacturer of said mobile computing device.

4. The method of claim 1, wherein said pool of addresses are assigned to a network interface of said mobile computing device by a manufacturer and are unknown to a third party.

5. The method of claim 1, wherein, when a user is to connect to an access point, a random address from said pool is provided, thereby allowing the user to connect to the access point.

6. The method of claim 5, wherein, when the user connects subsequently, a second address from the pool is used, said second address being different from said random address.

7. The method of claim 1, wherein said pool of addresses comprise non-contiguous addresses.

8. The method of claim 1, further comprising:

providing a block of subscriptions to a group, said group including said user, each subscription including its own user ID and password.

9. The method of claim 8, further comprising:

judging whether a user ID and password and an address have been used previously at a particular site by said user; and

based on said judging, subsequently selecting a different user ID and a different address at said particular site for said user.

10. The method of claim 5, further comprising:

overriding, by said user, an address provided for use for said user, and intervening such that the user selects a specific address to use in the pool.

11. The method of claim 1, further comprising:

sending an interactive message to the user.

12. The method of claim 1, wherein said network comprises a wireless network.

13. The method of claim 1, wherein said network comprises a wired network.

14. The method of claim 1, further comprising:

selectively adjusting a number of addresses in said pool made available to said user based on a level of service desired by said user.

15. The method of claim 1, further comprising:

selecting a random string for a user's host name each time said user logs on to an access point, such that the host name is unusable for location tracking.

16. A method of providing a connection to an access point to a network, comprising:

providing a detachable network interface for use in accessing said access point by a computing device,

said detachable network interface breaking a linkage between a media access control (MAC) address associated with said computing device and the user.

17. The method of claim 16, further comprising:

metering an amount of service at said access point used by said user.

18. The method of claim 16, further comprising:

placing a secret key on the detachable network interface.

19. The method of claim 18, wherein said secret key is placed on all detachable network interfaces.

20. The method of claim 18, wherein a different one of said secret key is provided for each said detachable network interface.

21. The method of claim 16, wherein said detachable network interface includes a balance display for indicating a balance representing an amount of service remaining on said detachable network interface, and thereby allowing for said detachable network interface to be tradable.

22. The method of claim 16, further comprising:

securely signing onto said network by said detachable network interface without a user performing any explicit action.

23. The method of claim 16, further comprising:

placing authentication information on said detachable network interface such that said network interface signs-on to obtain access to the network without explicit user action.

24. The method of claim 18, further comprising:

challenging the detachable network interface to determine if said detachable network interface contains the secret key.

25. The method of claim 24, wherein said challenging comprises generating a random number by the access point and sending the random number to the detachable network interface encrypted using the secret key.

26. The method of claim 25, further comprising:

authenticating the detachable network interface such that the number is decrypted, on the user side, using the secret key, transforming the number in a predetermined manner, re-encrypting the number and sending the number back to the access point.

27. The method of claim 26, wherein if the detachable network interface authenticates, then the user is allowed access to said access point.

28. The method of claim 18, wherein each detachable network interface contains a secret key unique from one another, said method further comprising:

maintaining a database of secret keys indexed by a media access control (MAC) address.

29. A system for providing location privacy, comprising:

a module for assigning a pool of addresses with which a user can access a network via a mobile computing device, so as to prevent a third party from correlating a user's location with the mobile computing device.

30. The system of claim 29, wherein said pool of addresses is issued by a manufacturer of said mobile computing device.

31. The system of claim 29, wherein, when a user is to connect to a certain access point, said module for assigning provides a random address from said pool, thereby allowing the user to connect to the access point.

32. The system of claim 31, wherein when the user connects again, said module for assigning provides a second address from the pool, said second address being different from said random address.

33. The system of claim 29, wherein said pool of addresses comprises non-contiguous addresses.

34. The system of claim 29, wherein a block of subscriptions is provided to a group, said group including said user, each subscription including its own user ID and password.

35. The system of claim 34, further comprising:

a module for judging whether a user ID and password and an address have been used previously at a particular site by said user; and

a module, based on an output of said module for judging, for subsequently selecting a different user ID and a different address at said particular site for said user.

36. The system of claim 29, further comprising:

a module for overriding the module for assigning and intervening such that the user selects a specific MAC address to use of the pool.

37. The system of claim 29, further comprising:

a module for sending an interactive message to the user.

38. The system of claim 29, wherein said network comprises a wireless network.

39. The system of claim 29, wherein said network comprises a wired network.

40. The system of claim 29, further comprising:

a module for selectively adjusting a number of addresses in said pool made available to said user, based on a level of service desired by said user.

41. The system of claim 29, further comprising:

a module for selecting a random string for a user's host name each time said user logs on to an access point, such that the host name is unusable for location tacking.

42. A system for providing a connection to an access point to a network, comprising:

a detachable network interface for use in accessing said access point by a computing device,

said detachable network interface breaking a linkage between a media access control (MAC) address associated with said computing device and the user.

43. The system of claim 42, further comprising:

a module for metering an amount of service at said access point used by said user.

44. The system of claim 42, further comprising:

a secret key placed on the detachable network interface.

45. The system of claim 44, wherein said secret key is placed on all detachable network interfaces.

46. The system of claim 44, wherein a different one of said secret key is provided for each said detachable network interface.

47. The system of claim 42, wherein said detachable network interface includes a balance display for indicating a balance representing an amount of service remaining on said detachable network interface, and thereby allowing for said detachable network interface to be tradable.

48. The system of claim 42, wherein said detachable network interface securely signs onto the network without a user performing any explicit action.

49. The system of claim 42, further comprising:

authentication information on said detachable network interface such that said network interface signs-on to obtain access to the network without explicit user action.

50. The system of claim 44, further comprising:

a module for challenging the detachable network interface to determine if said detachable network interface contains the secret key.

51. The system of claim 50, wherein said module for challenging comprises a generator for generating a random number by the access point and sending the random number to the detachable network interface encrypted using the secret key.

52. The system of claim 51, further comprising:

a module for authenticating the detachable network interface such that the number is decrypted, on the user side, using the secret key, transforming the number in a predetermined manner, re-encrypting the number and sending the number back to the access point.

53. The system of claim 52, wherein if the detachable network interface authenticates, then the user is allowed access to said access point.

54. The method of claim 42, wherein each said detachable network interface contains a secret key unique from one another, said system further comprising:

a module for maintaining a database of secret keys indexed by a media access control (MAC) address.

55. A method for deploying computing infrastructure, comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing the method of claim 1.

56. A method for deploying computing infrastructure, comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing the method of claim 16.

57. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform the method of claim 1.

58. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform the method of claim 16.